What is claimed is:

1. A data administration method, which comprises:

preparing a real data section by encrypting digital content to be distributed;

preparing a header data section provided with symbol information symbol-converted for visual or auditory recognition of attributes of the digital content;

preparing a consent-information-added header data section in which consent information containing information on a content key used as an encryption key in encrypting the digital content is embedded in the header data section as an electronic watermark; and

preparing composite data in which the real data section and the consent-information-added header data section are composited, and distributing the composite data.

2. The data administration method as set forth in claim 1, wherein said header data section is made by compositing into one image data item more than one image-symbol data item symbol-converted for visually recognizing attributes corresponding respectively to a plurality of digital content items.

3. A data administration method, which comprises:

preparing a real data section by encrypting digital content to be distributed;

preparing a header data section enabling visual or auditory recognition of substance of the digital content;

preparing a consent-information-added header data section in which consent information containing information on a content key used as an encryption key in encrypting the digital content is embedded in the header data section as a visually or auditorily unrecognizable electronic watermark;

preparing an annex data section in which use restriction information for restricting use of the digital content is encrypted;

preparing composite data by compositing the real data section and the consent-information-added header data section, simultaneously compositing the annex data section; and

distributing the composite data.

4. The data administration method as claimed in claim 3, wherein the use restriction information is embedding logic for embedding the consent information as the electronic watermark in the header data section.

5. The data administration method as set forth in claim 3, wherein the use restriction information is based on a use term during which, or on a use count up to which, the digital content is usable.

6. The data administration method as set forth in claim 3, wherein the use restriction information is encrypted

with, as an encryption key, personal information on a user of the digital content.

7. The data administration method as set forth in claim 6, wherein the encryption key when encrypting the use restriction information is a password preset by the user.

8. The data administration method as set forth in claim 6, wherein the encryption key when encrypting the use restriction information is identifying information specific to a recording medium in which the composite data is recorded.

9. The data administration method as set forth in claim 6, wherein the encryption key when encrypting the use restriction information is vital information on the user.

10. A data administration method, which comprises:

separating an annex data section from composite data distributed as a composite of

a real data section in which digital content to be distributed is encrypted,

in a header data section enabling visual or auditory recognition of substance of the digital content, a consent-information-added header data section in which consent information containing information on a content key used as an encryption key in encrypting the digital content is embedded as a

visually or auditorily unrecognizable electronic watermark, and

an annex data section in which use restriction information for restricting use of the digital content is encrypted;

decrypting the annex data section and extracting the use restriction information;

extracting the consent information embedded in the consent-information-added header data section based on the use restriction information;

obtaining from the consent information a content key for decrypting the digital content; and

using the content key, decrypting the real data section into its original digital content to allow use by users.

11. A data administration method characterized by:

preparing a real data section by encrypting digital content to be distributed;

preparing a header data section enabling visual or auditory recognition of substance of the digital content;

preparing a consent-information-added header data section in which consent information containing information on a content key used as an encryption key in encrypting the digital content is embedded in the header data section as a visually or auditorily unrecognizable electronic watermark;

embedding in the header data section as a visually or auditorily unrecognizable electronic watermark a hash value generated from the real data section using a hash function; and thereafter

preparing composite data in which the real data section and the consent-information-added header data section are composited, and distributing the composite data.

12. A data administration method characterized by:

preparing a real data section by encrypting digital content to be distributed;

preparing a header data section enabling visual or auditory recognition of substance of the digital content;

preparing a consent-information-added header data section in which consent information containing information on a content key used as an encryption key in encrypting the digital content is embedded in the header data section as a visually or auditorily unrecognizable electronic watermark; and

decrypting the real data section into digital content for sending out, by line-connecting to a predetermined contact destination, content information from the digital content that is decrypted, and therein

embedding in the header data section as a visually or auditorily unrecognizable electronic watermark the content information from the digital content that is

decrypted and information on the predetermined contact destination; and thereafter

preparing composite data in which the real data section and the consent-information-added header data section are composited, and distributing the composite data.

13. A data administration method characterized by:

preparing a real data section by encrypting digital content to be distributed;

preparing a header data section enabling visual or auditory recognition of substance of the digital content;

preparing a consent-information-added header data section in which consent information containing information on a content key used as an encryption key in encrypting the digital content is embedded in the header data section as a visually or auditorily unrecognizable electronic watermark;

preparing composite data in which the real data section and the consent-information-added header data section are composited, and therein retaining within the composite data record-location information from a server in which the digital content is registered; and

distributing the composite data.

14. The data administration method as set forth in claim 13, characterized in that the record-location information from the server in which the digital content is

registered is embedded in the header data section as a visually or auditorily unrecognizable electronic watermark.

15. A data administration method characterized by:

preparing a real data section by encrypting digital content to be distributed;

preparing a header data section enabling visual or auditory recognition of substance of the digital content;

preparing a consent-information-added header data section in which consent information containing information on a content key used as an encryption key in encrypting the digital content is embedded in the header data section as a visually or auditorily unrecognizable electronic watermark; and

preparing composite data in which the real data section and the consent-information-added header data section are composited, and therein retaining within the composite data vital template information generated based on vital information on a user of the digital content; and

distributing the composite data.

16. The data administration method as set forth in claim 15, characterized in that the vital template information is embedded in the header data section as a visually or auditorily unrecognizable electronic watermark.

17. A data administration method characterized by:

preparing a real data section by encrypting digital content to be distributed;

preparing a header data section enabling visual or auditory recognition of substance of the digital content;

preparing a consent-information-added header data section in which consent information containing information on a content key used as an encryption key in encrypting the digital content, and identifying information specific to a recording medium for recording the digital content, are embedded in the header data section as a visually or auditorily unrecognizable electronic watermark; and

preparing composite data in which the real data section and the consent-information-added header data section are composited, and distributing the composite data.

18. A data administration method characterized by:

preparing a real data section by encrypting digital content to be distributed;

preparing a header data section enabling visual or auditory recognition of substance of the digital content;

preparing a consent-information-added header data section in which consent information containing information on a content key used as an encryption key in encrypting the digital content, and a control code allowing a given operation on an information device for reproducing the digital content, are embedded in the header data section as

a visually or auditorily unrecognizable electronic watermark; and

preparing composite data in which the real data section and the consent-information-added header data section are composited, and distributing the composite data.

19. A data administration method, which comprises:

preparing a real data section by encrypting digital content to be distributed;

preparing a header data section enabling visual or auditory recognition of substance of the digital content;

preparing a consent-information-added header data section in which consent information containing information on a content key used as an encryption key in encrypting the digital content is embedded in the header data section as a visually or auditorily unrecognizable electronic watermark; and

preparing composite data by compositing the real data section and the consent-information-added header data section, and distributing the composite data; characterized in that

privileges information for the digital content including copyright information is embedded within the digital content as an electronic watermark.

20. The data administration method as set forth in claim 19, characterized in that morphology and code level of

the electronic watermark embedded in the digital content are determined based on a data quality level and a security level required by the digital content.

21. The data administration method as set forth in claim 19, characterized in that the electronic watermark embedding mode in the digital content differs from the electronic watermark embedding mode in the header data section.